软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2016,27(6):1328−1348 [doi: 10.13328/j.cnki.jos.005004]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

云计算环境安全综述*

张玉清[1], 王晓菲[1], 刘雪峰[2], 刘 玲[2]

[1](中国科学院大学 国家计算机网络入侵防范中心,北京 101408)

[2](综合业务网理论及关键技术国家重点实验室(西安电子科技大学),陕西 西安 710071)

通信作者: 张玉清, E-mail: zhangyq@ucas.ac.cn

摘 要: 伴随云计算技术的飞速发展,其所面临的安全问题日益凸显,在工业界和学术界引起了广泛的关注.传统的云基础架构中存在较高安全风险,攻击者对虚拟机的非法入侵破坏了云服务或资源的可用性,不可信的云存储环境增大了用户共享、检索私有数据的难度,各类外包计算和云应用需求带来了隐私泄露的风险.从云计算环境下安全与隐私保护技术的角度出发,通过介绍云虚拟化安全、云数据安全以及云应用安全的相关研究进展,分析并对比典型方案的特点、适用范围及其在安全防御和隐私保护方面的不同效用,讨论已有工作的局限性,进而指出未来发展趋势和后续研究方向.

关键词: 云计算;云安全;虚拟化安全;数据安全;应用安全

中图法分类号: TP309

中文引用格式: 张玉清,王晓菲,刘雪峰,刘玲.云计算环境安全综述.软件学报,2016,27(6):1328−1348. http://www.jos.org.cn/1000-9825/5004.htm

英文引用格式: Zhang YQ, Wang XF, Liu XF, Liu L. Survey on cloud computing security. Ruan Jian Xue Bao/Journal of Software, 2016,27(6):1328−1348 (in Chinese). http://www.jos.org.cn/1000-9825/5004.htm

Survey on Cloud Computing Security

ZHANG Yu-Qing[1], WANG Xiao-Fei[1], LIU Xue-Feng[2], LIU Ling[2]

[1](National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing 101408, China)

[2](National Key Laboratory of Integrated Services Networks (Xidian University), Xi'an 710071, China)

Abstract: With the rapid development of cloud computing technology, its security issues have become more and more obvious and received much attention in both industry and academia. High security risk is widespread in traditional cloud architecture. Hacking into a virtual machine destroys the availability of cloud services or resources. Un-Trusted cloud storage makes it more difficult to share or search users' private data. The risk of privacy leakage is caused by various outsourcing computation and application requirements. From the perspective of security and privacy preserving technologies in cloud computing, this paper first introduces related research progress of cloud virtualization security, cloud data security and cloud application security. In addition, it analyzes the characteristics and application scopes of typical schemes, and compares their different effectiveness on the security defense and privacy preserving. Finally, the paper discusses current limitations and possible directions for future research.

Key words: cloud computing; cloud security; virtualization security; data security; application security

云计算(cloud computing)是以网络技术、虚拟化技术、分布式计算技术为基础,以按需分配为业务模式,具备动态扩展、资源共享、宽带接入等特点的新一代网络化商业计算模式.开放的网络环境为云计算用户提供了

* 基金项目: 国家自然科学基金(61272481, 61402352, 61572460)
Foundation item: National Natural Science Foundation of China (61272481, 61402352, 61572460)
收稿时间: 2015-08-15; 修改时间: 2015-10-09; 采用时间: 2015-12-05; jos 在线出版时间: 2016-01-21
CNKI 网络优先出版: 2016-01-22 10:14:51, http://www.cnki.net/kcms/detail/11.2560.TP.20160122.1014.008.html

强大的计算和存储能力,现已逐渐在产业界得到广泛的应用.然而,伴随云计算技术的飞速发展,其所面临的安全问题日益凸显[1−3].

云计算环境是指将分布在互联网上的计算机等终端设备相互整合,借助某种网络计算方式,实现软硬件资源共享和协调调度的一种虚拟计算系统,具有快速部署、易于度量、终端开销低等特征.基本组成部分包括应用层、平台层、资源层、用户访问层以及管理层,并以各类云计算服务作为技术核心.因此在这种环境中,云计算用户的数据和资源完全依赖于不可靠的网络通信和半可信的云存储服务器,使得用户对云计算环境的安全性普遍存在质疑,导致云计算的普及难以深入.

一般认为,云计算环境自身的结构特点是造成安全问题的主要原因.首先,参与计算的节点种类多样、位置分布稀疏且通常无法有效控制.其次,云服务供应商(cloud service provider,简称 CSP)在传输、处理和存储的过程中均存在泄露隐私的风险.此外,由于云计算本质上是在现有技术的基础上建立的,所以已有技术的安全漏洞会直接转移到云计算平台上,甚至存在更大的安全威胁.可见,在云计算环境中,用户基本丧失了对私有信息和数据的控制能力,从而触发了一系列重要的安全挑战,例如:云端数据的存放位置、数据加密机制、数据恢复机制、完整性保护、第三方监管和审计、虚拟机安全、内存安全等.

鉴于安全和隐私保护是云计算发展的首要前提[4],也是目前科研工作的热点与焦点之一,本文将从云计算环境下安全与隐私保护技术的角度出发,综述云安全的研究进展.根据 NIST 在 2011 年公布的标准报告[5],本文将云安全划分为 3 个部分,分别是云虚拟化安全、云数据安全以及云应用安全,如图 1 所示.其中,云虚拟化安全主要研究对虚拟机、数据中心和云基础设施的非法入侵;云数据安全主要保护云存储数据的机密性、完整性与可搜索性;云应用安全主要包括外包计算、网络和终端设备的安全.

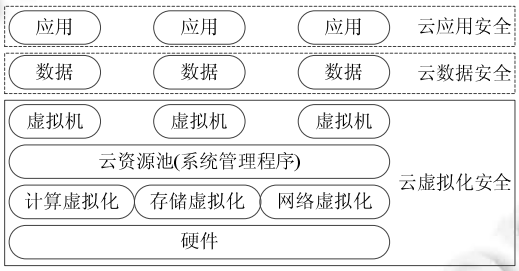


Fig.1 Cloud architecture and security classification

图 1 云基础架构与安全分类

本文试图通过介绍云虚拟化安全、云数据安全以及云应用安全的相关研究进展,分析并对比典型方案的特点、适用范围及其在安全防御和隐私保护方面的不同效用,讨论已有工作的局限性,进而指出未来发展趋势和后续研究方向.本文第 1 节~第 3 节分别从虚拟化、数据、应用 3 个方面综述云计算在安全方面的研究现状.第 4 节简要展望未来发展方向.最后是结束语.

1 云虚拟化安全

云计算平台对现有计算技术的整合是借助云虚拟化(cloud virtualization)实现的.云端的虚拟化软件将物理计算设备划分为一个或多个虚拟机(virtual machine,简称 VM),用户可以灵活调配虚拟机执行所需计算任务.例如:操作系统级虚拟化允许在相互独立的多台计算设备间创建可扩展的虚拟系统,此时闲置的计算资源得以重新分配,从而节约计算成本并提高资源利用率.

云虚拟化作为云计算的核心技术,其安全性至关重要.本节详述云虚拟化安全,重点介绍各类已知安全攻击及其现有防御技术,例如:窃取服务攻击可以非法窃取他人的云计算资源;恶意代码注入攻击、交叉虚拟机边信道攻击、定向共享内存攻击和虚拟机回滚攻击都会造成敏感信息泄露或未授权访问私有云资源.最后简要补充云计算硬件安全方面的研究情况.

1.1 已知安全攻击及防御技术

1.1.1 窃取服务攻击

公有云计算环境通常采用多种弹性计费模式,例如根据 CPU 或 VM 的总运行时间计费.然而,计费模式的周期性采样与低精度的时钟调度策略使得攻击者可以利用虚拟层调度机制的漏洞,使系统管理程序错误地检测 CPU 或 VM 用度,实现窃取服务攻击(theft-of-service attack).具体做法是确保攻击者进程在调度程序计数时未被调度,从而以隐蔽的方式占用他人的云服务资源.

常规的虚拟机调度机制没有对调度的正确性进行检查,是造成窃取服务攻击的主要原因.最初,Gruschka 与 Jensen 的工作[6]采用监控实例来保护调度安全,对比分析攻击者与合法实例之间的差异以识别窃取服务攻击.2013 年,Zhou 等人[7]则通过修改调度机制有效地防御了此类攻击,同时兼顾了计算效率、公平性与 I/O 响应能力.近期研究的目标是虚拟机最小化,包括对可信计算基[8]和虚拟机软件[9]的最小化,有助于减少受攻击面并保护用户隐私.

此外,2012 年提出的资源释放型攻击(resource-freeing attack,简称 RFA)[10]能够将合法用户的虚拟机资源非法转移到攻击者的虚拟机,从而达到与窃取服务攻击类似的攻击效果,而且目前并不存在可以完全避免这类攻击的可行方案.在 RFA 中,攻击者通过耗尽某些关键资源,迫使目标虚拟机终止正在进行的服务并释放已占用的资源,此时攻击者将利用新释放的资源来改善自身的性能.Amazon EC2 平台上的实验结果表明,攻击者借助 RFA 获得了 13%的性能提升.

1.1.2 恶意代码注入攻击

恶意代码注入攻击(malware injection attack)使用恶意实例代替系统服务实例处理正常的服务请求,进而获得特权访问能力,非法盗取证书信息或用户数据.与传统 Web 应用环境不同,云计算环境的虚拟化特征加剧了恶意代码注入攻击的安全威胁.云端的服务迁移、虚拟机共存等操作使得恶意代码的检测工作异常困难,目前仍然缺少对云服务实例完整性的有效检查方法.

现有防御方案的关键点是对包含恶意实例的计算节点的检测.文献[11]基于 PE 文件格式关系设计可追溯性检测方案,针对 HADOOP 平台检测恶意实例所在的主机,具有较高的检测率和较低的误报率.然而,该方案的检测开销较大,而且检测过程存在隐私泄露的可能性.2012 年,一种轻量级云移动终端反恶意软件系统[12]被提出,移动端恶意代码的检测效率得以改善.随后,Wei 等人[13]基于 DFA 评估技术检测加密文件的内容真实性,同样能够用于恶意代码扫描.

1.1.3 交叉虚拟机边信道攻击

交叉虚拟机边信道攻击(cross VM side channels attack)是一类常见的访问驱动攻击形式,要求攻击者与目标虚拟机使用相同的物理层硬件,二者交替执行.在交替执行的过程中可以推断出目标虚拟机的行为,识别出服务器主机的信息.攻击者首先借助恶意虚拟机访问共享硬件和缓存,然后执行预定的安全攻击,例如计时边信道攻击[14]、能量消耗的边信道攻击[15]、高速隐蔽信道攻击[16,17]等,最终导致目标虚拟机内的用户数据泄露.此类攻击一般难以留下痕迹或引发警报,因而能够很好地躲避检测.

具体来看,计时边信道攻击[14]通过测量不同计算任务的执行时间,成功获取用户与服务器的身份信息.能量消耗的边信道攻击[15]利用能量消耗日志开展攻击,可以帮助攻击者快速识别目标虚拟机系统管理程序的类型.此外,与标准通信信道不同,Wu 等人[16]首次在虚拟化 x86 系统中实现了高速隐蔽信道攻击.2015 年,Liu 的科研团队[17]围绕最后一级缓存(last-level cache,简称 LLC)提出了一种新型隐蔽信道攻击.无需依赖共享内存以及操作系统或虚拟机系统管理程序的漏洞,便可达到较高的攻击成功率.Inci 等人[18]则是通过 LLC 来检测主机托管,在 Amazon EC2 平台上完整恢复了 2 048 比特的 RSA 私钥.

现阶段针对交叉虚拟机边信道攻击的典型防御策略有密钥划分机制[19]和最小运行时间担保机制[20].前者将用户密钥划分为随机份额,并以周期性更新的方式将各个密钥份额存储于不同的虚拟机,有效防范利用交叉虚拟机边信道攻击窃取加密密钥的攻击行为.后者优化虚拟机调度机制以降低缓存共享的安全风险,规定在最小运行时间限制内不能预先占用 CPU 资源.

1.1.4 定向共享内存攻击

定向共享内存攻击(targeted shared memory)以物理机或虚拟机的共享内存或缓存为攻击目标,是恶意代码注入攻击与边信道攻击的基础.此类攻击的一个代表性方案[21]由 Rocha 和 Correia 于 2011 年提出,结合内部攻击访问虚拟机的内存转储数据,可能导致系统当前运行状态与用户隐私信息的泄露.

同样是关于虚拟机的内存安全,内存耗尽故障[22]严重危害着云计算平台的可用性.目前常规的防御手段是根据日志文件来监控内存,相比直接监控内核例程的方法,其故障检测效果较为有限.

1.1.5 虚拟机回滚攻击

在云虚拟化环境中,管理程序出于系统正常维护的目的,可以随时挂起虚拟机并保存系统状态快照.若攻击者非法恢复了快照,将会造成一系列的安全隐患,且历史数据将被清除,攻击行为将被彻底隐藏.

2012 年,Szefer 等人[23]最初提出禁用挂起恢复功能以抵御虚拟机回滚攻击(VM rollback attack).同年,该思路得以改进,研究人员[24,25]选用虚拟机审计日志和状态快照的哈希值作为合法性的判断条件,而无需禁用系统管理程序的基本功能.然而,上述方案均需要终端用户的参与及协调,灵活性较差.

1.1.6 小 结

云虚拟化作为多种技术的融合,为云端的资源管理、数据隐私保护带来了全新的安全挑战.第 1.1 节介绍了 5 类常见的虚拟机安全攻击,为了更加直观地分析并对比各个攻击的原理、特点与危害程度,表 1 围绕攻击实例、攻击原理、攻击效果、代表性防御方案以及现有研究的局限性进行了详细的总结归纳.

Table 1 Known security attacks on cloud virtualization

表1 已知云虚拟化安全攻击

攻击类别	攻击实例	攻击原理	攻击效果	防御方案	局限性
窃取服务攻击	资源释放型攻击[10]	调度机制错误检测 VM 用度	1. 不付费使用云服务 2. 窃取他人的云资源	文献[6–9]	1. 未检查调度正确性 2. 检测的准确性较低 3. 无法抵御 RFA 攻击
恶意代码注入攻击	–	上传恶意实例代替系统服务实例处理正常的服务请求	1. 证书信息泄露 2. 用户数据泄露 3. 虚拟机异常服务	文献[11–13]	1. 未检查实例完整性 2. 检测的开销较大 3. 可检测的种类单一
交叉虚拟机边信道攻击	计时边信道攻击[14] 能量消耗的边信道攻击[15] 高速隐蔽信道攻击[16,17]	VM 交替执行过程中识别出服务器主机信息	1. 用户数据泄露 2. 云服务器信息泄露	文献[19,20]	难以抵御计时边信道攻击、能量消耗的边信道攻击和各类隐蔽信道攻击
定向共享内存攻击	文献[21]	攻击物理机或虚拟机的共享内存或缓存	1. 用户数据泄露 2. 云服务器信息泄露 3. 引发其他类型攻击	文献[22]	1. 检测效果较差 2. 干扰对共享内存的正常访问
虚拟机回滚攻击	–	非法恢复 VM 状态快照	1. 用户数据泄露 2. 破坏云基础设施 3. 隐藏攻击痕迹	文献[23–25]	1. 依赖于用户的交互 2. 干扰管理程序功能

综上所述,云虚拟化安全的研究已经取得了一些进展,但总体来说防御技术还不成熟,仍有众多针对虚拟机环境的安全攻击形式尚待深入研究.虚拟机迁移过程中的信息泄露、为窃取用户数据或服务资源而对虚拟机实例进行的非法调度、替换、回滚等操作,均是未来研究中十分值得关注的重要问题,需要设计更加完备的安全防御机制以保障虚拟机调度机制的可靠性.

1.2 云硬件安全

硬件设备安全是云基础架构安全不可或缺的重要组成部分,硬件的瞬时故障或错误可能危害整体信息系统的正确性与安全性.Elphinstone 等人[26]在形式化软件验证的基本假设下,分析商用硬件的可靠性特征,并利用冗余的多核处理器提高现有硬件的可信度.此外,与传统的软件安全技术不同,硬件系统的引入为云计算带来了一种全新的安全防护策略.例如:硬件安全模块(hardware security module,简称 HSM)负责存储并管理用于认证和加密的私有密钥,具有极高的加解密运算速度和安全保护级别,且易于与其他网络设备相整合.目前最著名的

商业化产品是亚马逊公司的 CloudHSM 服务,主要为 AWS 云提供密钥管理功能.类似地,Azab 等人[27]设计出独立于操作系统软件的硬件级强化隔离框架,旨在为 x86 多核平台的数据隐私提供必要保障.

虽然硬件安全的发展在一定程度上受到低性价比的限制,同时为了克服安全硬件在灵活性和可扩展性等方面的局限性,CSP 更倾向于使用软件架构代替硬件设备以获取更为优质的服务能力.但是即便如此,安全硬件对服务可靠性的提升却为用户带来了更多节省计算成本的机会.例如:基于硬件的身份认证机制通过将安全策略植入硬件模块来保护数据安全,使用户可以在确保隐私的前提下将过多的数据外包至云端,从整体上降低了用户安全防护和计算的开销.

2 云数据安全

不同于传统的计算模式,云计算在很大程度上迫使用户隐私数据的所有权与控制权相互分离.云存储作为云计算提供的核心服务,是不同终端设备间共享数据的一种解决方案,其中的数据安全已成为云安全的关键挑战之一,在近期研究中占有较大的比重.

本节回顾云计算环境中的数据安全与内容隐私保护的相关问题与研究进展.到目前为止,保护云数据安全的常规做法是预先对存储到云服务器的数据进行加密处理,并在需要时由数据使用者解密.在此过程中,代理重加密算法与属性加密算法用于解决数据拥有者与使用者之间的身份差异;访问控制技术用于管理资源的授权访问范围;可搜索加密技术实现对密文数据的检索.最后,为防备因 CSP 系统故障而导致的用户数据丢失,还需给出关于数据完整性以及所有权的证明.针对上述研究内容,本节将从数据共享算法、访问权限认证、密文搜索和完整性审计 4 个方面展开综述,并选取部分重点成果予以介绍和分析.

2.1 数据共享算法

2.1.1 代理重加密算法

代理重加密算法(proxy re-encryption,简称 PRE)常见于电子邮件转发、内容分发服务等多用户共享的云安全应用中,它允许第三方代理改变由数据发送方加密后的密文,以便数据接收方可以解密.最简单的做法是由第三方代理使用发送方密钥先行解密出明文,再以接收方密钥重新加密.但是对于不可信的 CSP 代理而言,该方案会造成密钥及明文信息的泄密,安全性并不理想.代理重加密的一般化流程如图 2 所示.

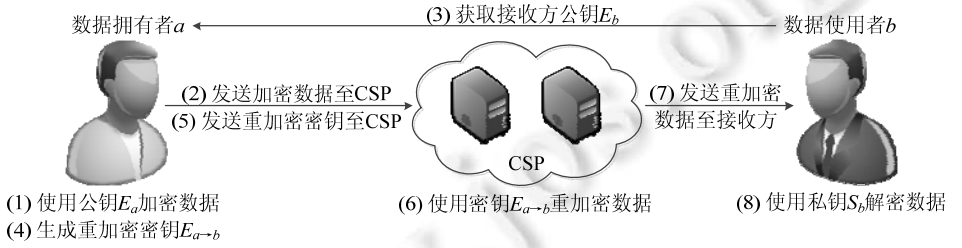


Fig.2 Process of proxy re-encryption

图 2 代理重加密流程

结合传统代理重加密算法的基本思想,Green 与 Ateniese 于 2007 年设计了一种基于身份的代理重加密方案(identity-based proxy re-encryption,简称 IBPRE)[28].此方案以用户的唯一身份信息作为公钥参与重加密,具有单向性、非传递性、非交互性等特点.其中所含的重加密密钥只能单向单次使用,而且无法抵御代理与接收方之间的合谋攻击.Mizuno 和 Doi 对 IBPRE 方案进行改进[29],优化了重加密密文空间的大小并隐藏了代理的身份,一并给出了严格的形式化安全分析,证明其具有抵抗选择明文攻击(chosen-plaintext attack,简称 CPA)的能力.2012 年,综合运用层次化身份加密算法 NaHIBE[30]和基于身份的多用单向代理重加密算法 MUIBPRE[31],首个可以抵御非法合谋且满足选择密文攻击(chosen-ciphertext attack,简称 CCA)安全的 IBPRE 方案被提出[32].除此之外,分类代理重加密技术[33]使数据分发者能够对密文委托权实施细粒度的分类控制.Wu 等人[34]则给出了

无证书的代理重加密算法以及基于身份的密钥托管协议.2014 年,基于身份的可撤销代理重加密机制[35]也得到了进一步的研究.总体上,IBPRE 方案解决了第三方代理权限过大的问题,但其所支持的委托方式较为单一,难以灵活地根据共享的内容分配解密能力.

条件代理重加密算法(conditional proxy re-encryption,简称 CPRE)[36]规定仅当重加密密钥和指定密文条件同时满足时,解密操作才被允许,特别支持一对多加密和端到端加密形式.在文献[36]的基础上,Fang 等人先后设计了支持关键词检索的匿名 CPRE 方案[37]和模糊 CPRE 方案[38],在执行效率上优于原始算法.期间,Lan 等人[39]利用秘密共享机制和双线性对原理构造出多条件代理重加密方案.与文献[32]的设计思想类似,文献[40]表明,多数层次化身份加密方案(hierarchical identity-based encryption,简称 HIBE)可以转化为 CCA 安全的 CPRE 方案.而基于身份的条件代理重加密方案则是由 IBPRE 和 CPRE 所组成的扩展算法,其 CCA 安全性已在标准模型(standard model)[41]和随机预言模型(random oracle model)[42]下得到充分的证明.然而,现有的方案大多仅限于关键字条件,如何构造支持布尔条件的 CPRE 算法仍然是一个开放的问题.此外,该类方案的效率与密文长度仍待进一步优化.

2.1.2 属性加密算法

云存储中,属性加密算法(attribute-based encryption,简称 ABE)同样可以保护用户数据的安全性与可共享性.若公钥密码的密钥与密文依赖于用户自身的某些属性(如性别、年龄、国籍、学历等),则称其为基于属性的加密算法或模糊的基于身份的加密算法(fuzzy identity-based encryption).此时仅当密钥属性与密文属性相互匹配时,才可以完成解密操作.

实现属性加密的方式多种多样,近期的代表性成果包括:Waters 所提出的基于密文策略的属性加密方案(ciphertext-policy attribute-based encryption,简称 CP-ABE)[43]最初用来解决复杂的密文访问控制问题.密文负责携带访问控制策略,因此加密时间与访问控制结构的复杂度呈现正相关,而解密时间由访问控制树中的节点总数目决定.文献[44]指出将部分解密算法外包到 CSP,可以有效降低 CP-ABE 方案的解密开销.然而,外包解密通常不具有可验证性,即用户无法判断 CSP 是否按照预定要求进行了解密转换.为了弥补这一缺陷,Lai 等人[45]在其 2013 年的工作中首次为 CP-ABE 设计了可验证的外包解密算法,但是可扩展性较差.此外,关于用户属性撤销或密钥更新问题,最新解决思路是使用直接撤销机制[46]或将 CSP 代理的计算任务分散到大量云计算用户中[47],以避免因间接属性撤销而导致的性能瓶颈.

2006 年,Goyal 等人[48]提出了基于密钥策略的属性加密方案(key-policy attribute-based encryption,简称 KP-ABE),将单调访问控制结构直接嵌入解密密钥,只有拥有特定密钥的用户可以解密数据.与 CP-ABE 算法类似,KP-ABE 算法的密文规模仍然受到属性数目的影响.为此,一系列具有固定密文长度的 KP-ABE 方案被陆续构造[49,50],其中解密操作所包含的双线性对运算的次数已降至常量级[51],从而减小了数据使用者的计算开销.2015 年,Ambrosin 等人[52]着力研究并通过实验验证了 ABE 应用于移动平台上的可行性.当用户属性或访问控制策略发生变化时,如何高效地更新解密密钥,是 KP-ABE 方案的遗留问题之一,目前尚未出现完备的解决方案.

2.1.3 小 结

代理重加密算法和属性加密算法为云存储数据的安全共享提供解决方案,现有研究的主要缺陷有:

(1) 代理重加密算法中,数据拥有者将加密后的数据上传至第三方代理.若此后云存储系统中的数据使用者的身份发生变化,或者数据共享策略出现动态更新,则代理方的数据管理工作将会异常复杂,且极易导致用户隐私数据的泄露,未来值得加强研究.

(2) 属性加密算法特别适合云计算的分布式架构,可以降低网络通信开销且便于与其他安全技术相结合.传统的属性加密算法在实际应用时遇到了一些新的问题,近期的研究成果允许用户的动态加入,能够抵御恶意节点的合谋攻击,同时支持包含布尔表达式的访问策略.然而,几乎所有的属性加密方案均借助可信机构生成密钥,因此仅适用于私有云计算环境,如何摆脱这一限制是未来研究的关键点.

2.2 访问控制技术

用户将私有数据存储到公有云服务器,数据的机密性容易受到外部与内部攻击的威胁.因此,对云数据中

心的访问需要经过严格的安全认证过程.访问控制(access control)包括授权、认证、访问认可、审计追踪 4 个基本环节.具体而言,授权用于划定主体的访问级别;认证操作负责验证数据使用者是否具备合法的访问权限,通常采用口令、生物扫描、物理密钥、电子密钥等认证方式;访问认可环节基于授权策略赋予用户实际访问资源的权利;审计追踪记录访问轨迹,用于事后问责.

动态、分布式的网络环境使得云计算平台的访问控制方案必须具有高度的可扩展性、灵活性与高效性.目前云端提供的权限管理机制存在一些普遍的问题[53],主要是如何确信 CSP 未将访问权限非法授予其他用户;如何在数据过期后安全地回收数据访问权以及如何克服意外或故意的访问冲突.2012 年,Leandro 等人[54]利用 Shibboleth 框架为云计算设计出无需可信第三方的多租户授权系统.该系统允许用户按照自身需要灵活修改安全策略,实现了严密的权限管理过程,但是口令认证机制的安全性较差,无法完全确保用户接入系统的合法性.原因在于云计算用户并非归属于单一的控制系统,而很可能会借助移动设备或应用软件从多个 CSP 处同时获取服务,所以现有的认证机制无法直接应用于云计算环境.

云计算一般采用动态策略的访问控制模型,属性加密及其扩展算法是其中重要的组成部分.Kuhn 等人[55]将基于角色的访问控制(role-based access control,简称 RBAC)与基于属性的访问控制(attribute-based access control)相结合.角色视作属性的一部分,在快速认证的同时支持动态的权限管理.风险感知的访问控制模型[56]进一步克服了 RBAC 机制在动态云环境中的功能性缺陷.令风险因素参与访问控制决策,均衡分析因认可未授权访问而带来的安全风险以及因拒绝授权访问而造成的不可用性,设定风险阈值为风险应用需求提供安全访问方案.2014 年提出的一种新型代理重加密算法[57]解决了一对多的云存储访问控制问题.仅将部分密文存储于云服务器,使数据发送方可以控制密文的传递范围,并降低了通信过程中的数据计算量和交换量.此外,研究人员[58]在 $UCON_{ABC}$ 使用控制模型下结合弹性授权重评估技术预测云服务的消耗量,并以此为依据实施服务计费和细粒度访问控制.

综上,访问控制技术在保护云数据机密性方面有着重要的作用,主要用于避免 CSP 和未授权用户的非法访问.能否根据多样的安全策略实现对外包数据的授权访问是云访问控制技术面临的核心挑战.代理重加密、属性加密与细粒度访问控制是 3 类常见的控制方法,近期则有一些结合不经意传输和匿名证书的新型访问控制技术被陆续提出.伴随云环境中日益严峻的隐私保护需求,未来研究将侧重于以下内容:

(1) 加强对多级访问控制和组群访问控制的研究,使不同权限的用户获得不同的访问能力.对于当前的研究成果,如果用户离开系统或用户等级变动,为避免出现未授权访问,必须对密钥进行更新,故灵活性有待改善.

(2) 访问控制应不仅仅局限于读权限,而是更多地向写权限转变,从而更加全面地保护云存储安全.

(3) 围绕新兴的跨云访问控制中的非法授权、访问权回收、访问冲突等问题而展开的有关研究.

2.3 可搜索加密技术

云存储采用可搜索加密技术(searchable encryption)保障数据的可用性,支持对密文数据的查询与检索,主要包括对称可搜索加密技术和非对称可搜索加密技术.密文搜索的一般化流程如图 3 所示.

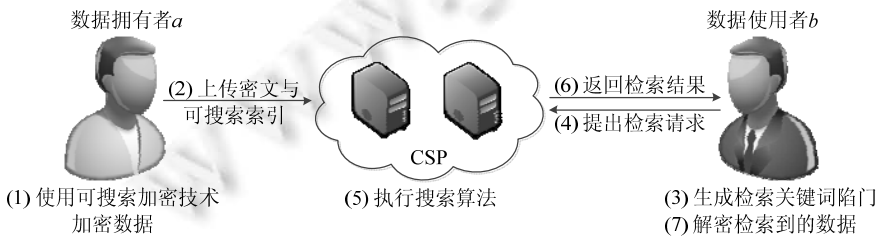


Fig.3 Process of searchable encryption

图3 密文搜索流程

数据拥有者将加密后的数据以及对应的可搜索索引上传至 CSP,数据使用者随后向 CSP 提出检索请求并

发送关键词陷门,最终由 CSP 安全地返回(排序后的)检索结果.该过程需确保 CSP 未窃取到任何与检索操作有关的额外信息.

2.3.1 对称可搜索加密技术

对称可搜索加密技术(symmetric searchable encryption,简称 SSE)的主流构造方式是建立索引.构造过程分为加密数据文件与生成可搜索索引两个阶段.一方面,数据拥有者使用标准对称加密算法对任意形式的数据文件进行加密处理,并存储于云服务器内,只有拥有对称密钥的用户有权解密访问.另一方面,数据拥有者使用特定的可搜索加密机制构建安全加密索引,在文件与检索关键词之间建立检索关联,并上传至云服务器以待关键词查询.此后在密文搜索时,由数据拥有者为数据使用者提供陷门,最终完成检索.

起初,对称可搜索加密技术的检索效率较差,检索时间与密文数据总长度呈现线性增长关系[59].数年来,围绕密文搜索效率的优化研究已经取得了实质性的突破,目前最优的安全范围查询方案[60]能够达到对数时间复杂度.近期,Strizhov 与 Ray 又提出了多关键词的相似性可搜索加密方案 MKSim[61],检索时间与命中文档总数之间存在亚线性关系.然而,上述方案均基于数据源集中化假设,即由单一数据源集中创建可搜索索引,而这与云计算的分布式特点相矛盾.2015 年,Liu 等人[62]为多数据源的场景设计了 MDS-SSE 算法,允许各数据源以分散的方式生成索引.该算法成功地保护了数据文件和检索结果的隐私,却泄露了数据源数目、数据文件数目以及访问模式和搜索模式等信息.Li 等人[63]利用云存储系统的 CP-ABE 技术实现对部分接入结构的隐藏,并分别在 DBDH 假设和 DL 假设下给出了安全性证明.Rompay 等人[64]则构造出能力更强的敌手模型,探讨并防御多用户检索过程中的合谋攻击问题.其中,大量双线性对的运算限制了检索效率,带来了较大的运算和通信开销,且检索精度较低.

2.3.2 非对称可搜索加密技术

非对称可搜索加密技术(asymmetric searchable encryption,简称 ASE)解决了服务器不可信与数据来源单一等问题.该项技术保留了非对称加密算法的特性,允许数据发送者以公钥加密数据与关键词,而数据使用者则利用私钥自行生成陷门以完成检索.

Boneh 等人[65]基于公钥密码体制提出的 PEKS 算法是非对称可搜索加密技术研究的开端.PEKS 算法支持合取查询、子集查询和范围查询,但其陷门加密方式易受推理攻击的威胁.Baek 等人[66]给出了初步的应对策略,但是由于引入了关键词合取技术,导致加密运算时间显著延长.谓词加密[67]也是一类有效的安全检索技术,常见于析取等数据查询操作.不同于 SSE 技术,已知的非对称可搜索加密方案通常难以提供多关键词检索功能.关于模糊关键词检索,INFOCOM 2010 年的一项研究[68]利用字符串编辑距离算法衡量关键词之间的相似度,从而构造出包含通配符的安全查询机制.

2.3.3 小 结

总体上来说,面对云存储的海量数据,当前的研究热点是如何令可搜索加密技术支持多关键词检索和相关性排序,同时进一步提高检索速度与精度,并降低运算与通信开销.具体来看,后续研究应重点解决以下问题:

(1) 对称可搜索加密技术应用于大规模数据集时的检索性能显著下降,常规解决方法是预计算可搜索索引,随之而来的是索引的安全问题.未来研究应支持更多类型的查询表达式,例如短语搜索、邻近搜索和正则表达式等.此外,扩展密文搜索的应用范围,特别是对外包数据库、加密电子邮件等信息的安全检索.

(2) 基于关键词的非对称可搜索加密技术存在的主要局限性是检索效率的问题,并且缺乏多用户环境下的可扩展能力.因此未来工作的目标之一是降低加解密计算的复杂性,设计更加高效且安全的密文搜索方案.

2.4 可回收性与所有权证明

据云安全联盟公布的最新报告显示,数据丢失是云计算中排名第二的安全威胁[69].用户在使用云存储数据之前,应对数据的完整性进行验证.可回收性证明(proofs of retrievability,简称 PoR)[70]是一类知识证明协议,于 2007 年被首次提出.由 CSP 向数据拥有者证明目标文件可以被完整取回.Zeng 围绕该思路进行优化,构造了基于双线性对的可证明数据完整性方案 PDI[71].突出贡献是其所具备的公开可验证性,即允许第三方验证者进行验证,从而有效降低了数据使用者的验证开销,但是数据拥有者产生验证标记的计算复杂度依然很高.2014 年,

OPoR 方案[72]的出现很好地解决了上述问题.在该方案中,半可信的第三方审计服务器在预处理阶段按照用户要求生成验证标记,从根本上减轻了用户的计算负担.此外,基于有状态 MAC 树[73]、BLS 同态签名[74]等技术,也出现了许多完整性验证机制.

数据所有权的证明(provable data possession,简称 PDP)[75]同样可以公开验证云端数据的完整性.由于验证过程中服务器的数据量和通信量较小,因此 PDP 模型适用于大规模分布式存储系统.当数据以多副本的方式存储于 CSP 时,用户需要对副本的个数与一致性进行额外的判断.为此,Barsoum 等人[76]提出了相应的解决方案 MB-PMDDP,同时能够抵御服务器合谋并支持动态的数据更新.类似地,基于身份的分布式数据完整性检测模型 ID-DPDP[77]针对数据存储于不同云服务器的情况,实现了私有验证、委托验证和公开验证.

综上所述,适用于云环境的数据完整性验证技术已经得到了广泛的研究.数据使用者希望尽可能提高验证效率并降低验证开销,或者将数据完整性的定期审计工作委托给第三方机构,此时可回收性证明应具备公开可验证性.最新的研究内容以及局限性包括:

(1) 通信复杂度一般与验证数据规模线性相关,故当可用带宽资源有限时,应设法降低验证方案的通信量.

(2) 完整性验证者的存储开销和密钥管理难度较大,所需的验证计算量随数据规模增长,难以有效控制.

(3) 防御服务器合谋伪造、多数据源或动态数据更新条件下的所有权证明等,有望成为未来的研究重点.

3 云应用安全

各类云应用自身的安全性直接关乎云计算产业未来的发展,因此尤为重要.对于基于云的各类应用,如网页操作系统、数据库管理系统、数据挖掘算法的外包协议等,首先需要预防应用本身固有的安全漏洞,同时设计针对性的安全与隐私保护方案提高应用安全性.本节分析云计算应用在技术层面面临的安全威胁,包括拒绝服务攻击、僵尸网络攻击和音频隐写攻击等.随后重点介绍两类可计算加密技术,并进一步探讨其在隐私保护外包计算和可验证外包计算中的重要应用.最后简略概述其他云应用安全问题.

3.1 已知安全攻击及防御技术

3.1.1 拒绝服务攻击

拒绝服务攻击(denial-of-service attack,简称 DoS)是计算机网络中一类简单的资源耗尽型攻击,攻击者向目标主机发起大规模处理请求,试图耗尽系统资源,致使正常的软硬件服务瘫痪.具体到云计算环境,云计算资源的集中分配方式使得拒绝服务攻击的破坏程度进一步加剧,攻击者的首选目标已从过去的密集基础设施转变为关键的云服务程序.相比底层的窃取服务攻击,常见的拒绝服务攻击主要针对上层的云计算应用,特别是以 SaaS(software-as-a-service,软件即服务)平台为代表的各类软件服务.由于目前已知的上层应用大多通过网页浏览器接入,故攻击难度通常更小,攻击范围通常更大,对云应用安全的威胁也更加显著.

云端的(分布式)拒绝服务攻击主要存在 3 类具体的攻击形式,分别基于 XML、HTTP 和 REST 技术,其中 XML 和 HTTP 广泛存在于云计算的各类应用中,针对这两种协议发动的 DoS 攻击具有更强的针对性和破坏能力.现有防御策略大多源于过滤技术.2012 年,Karnwal 等人[78]使用 5 种过滤技术成功检测基于 HTTP 和 XML 的分布式拒绝服务攻击.由于该方法逐条过滤各节点的通信报文,导致通信速率有所降低.此外,针对云计算的按需计费模式,欺骗性资源耗尽攻击(fraudulent resource consumption attack)[79]是云计算环境中特有的一种拒绝服务攻击,通过消耗目标主机所购置的带宽资源,给用户带来严重的经济负担.

3.1.2 僵尸网络攻击

僵尸网络攻击(botnets attacks)中,攻击者操纵僵尸机隐藏身份与位置信息实现间接攻击,从而以未授权的方式访问云资源,同时有效降低被检测或追溯的可能性.近年来,Amazon EC2、Google App Engine 等多家云计算平台相继出现僵尸网络攻击.原因在于弹性的计算资源与灵活的访问方式为僵尸网络提供了良好的运行环境,攻击者一方面可以使用云服务器作为主控机,另一方面也可以使用窃取到的高性能虚拟机作为僵尸机.最新的攻击方案[80]利用推送通知服务的缺陷来发送控制命令,在 Android 平台组建移动僵尸网络推送垃圾邮件.

检测僵尸网络的首要工作是识别僵尸网络通信的加密密钥,进而追溯出僵尸主控机,而现有研究成果[81]却

难以监测使用非对称密钥加密的僵尸网络流量.云虚拟机的数据包自动过滤机制[82]同样可以用于发现僵尸网络攻击,但是无法阻止对合法应用行为的错误过滤.

3.1.3 音频隐写攻击

2015 年,Hasna 创造性地在混合云计算环境中使用音频隐写技术代替加密算法完成数据隐藏任务[83].然而,攻击者则利用该项技术欺骗安全机制,将恶意代码隐藏于音频文件并提交至目标服务器.此类攻击称为音频隐写攻击(audio steganography attack),通常会导致云存储系统出现严重的故障.

文献[84]提出 StegAD 方案,包含增强型 RS 算法和 SADI 算法.其中,增强型 RS 算法负责检测恶意音频隐写文件,随后交由 SADI 算法推断出可能的代码隐藏位置.该方案的局限性在于携带恶意代码的音频文件与合法音频文件难以相互区分.

3.1.4 小 结

对于云服务供应商与云计算用户而言,云应用安全都是一个十分重要的问题.在第 3.1 节中,先后介绍了 3 类常见的云应用安全攻击,为了更加直观的分析并对比各个攻击的原理、特点与危害程度,表 2 围绕攻击实例、攻击原理、攻击效果、代表性防御方案以及现有研究的局限性进行了详细的总结归纳.

Table 2 Known security attacks on cloud application

表2 已知云应用安全攻击

攻击类别	攻击实例	攻击原理	攻击效果	防御方案	局限性
拒绝服务攻击	XML based DoS HTTP based DoS REST based DoS 分布式拒绝服务攻击 欺骗性资源耗尽攻击[79]	向目标主机发起大规模处理请求以耗尽系统资源	1. 软硬件服务瘫痪 2. 未授权访问 3. 用户数据泄露	文献[78]	1. 过滤技术干扰通信 2. 无法完全避免分布式 DoS 攻击 3. 难以抵御欺骗性资源耗尽攻击
僵尸网络攻击	文献[80]	僵尸主控机操纵僵尸机实现间接攻击	1. 未授权访问 2. 用户数据泄露 3. 云服务异常	文献[81,82]	1. 干扰合法应用行为 2. 检测降低网络性能
音频隐写攻击	–	将恶意代码隐藏于音频文件并提交至目标服务器	1. 破坏云存储系统 2. 用户数据泄露	文献[84]	干扰合法的音频隐写

云计算各类应用的安全性在很大程度上依赖于其所属网络的安全环境,因此网络协议中存在的安全漏洞将导致一系列针对云应用的安全攻击,并因云计算的结构特点而不断恶化.在部署云应用环境的同时,需要做好已知应用安全攻击的防御工作,从而保护云基础服务的安全性与用户的数据隐私.

3.2 隐私保护外包计算

3.2.1 同态加密技术

全同态加密(fully homomorphic encryption,简称 FHE)是一种允许直接对密文进行操作的可计算加密技术.CSP 根据密文完成计算后,用户解密该密文计算结果,即可获得对应明文的运算结果.

2009 年,IBM 公司的 Gentry 在全同态加密技术方面取得了重大的突破[85].Gentry 依据理想格的计算复杂性理论,构造出首个语义安全的全同态加密算法,支持加法同态和乘法同态.但是该算法实现复杂,加解密效率低,难以实用化.随后,在此工作基础上,相关学者不断完善同态加密算法,寻找性能优化的有效方式,主要围绕不同应用需求展开深入探究.

2011 年前后,Brakerski 与 Vaikuntanathan 等人给出了基于纠错学习假设的同态加密方案[86,87],结合密钥交换技术和模交换技术降低密文噪声,从而改善算法效率,极大地推进了同态加密技术的快速发展.此后的一项研究[88]便利用 FHE 技术实现了全同态消息认证机制.类似地,Boneh 与 Freeman 首次提出多项式环上的全同态签名[89].这一结论于 2014 年被 Dario 等人[90]进一步完善,无需依赖随机预言模型,可以达到更高的安全性,而且签名验证效率有所提高.

然而,目前全同态加密技术的真实性能与实际应用之间依然存在着较大的差距,更无法确保加密计算结果的正确性,而是需要额外整合某些高效的结果验证机制.相比之下,类同态加密技术(somewhat homomorphic

encryption,简称 SWHE)的加解密性能较优,但是仅适用于低阶多项式运算,即只允许有限次数的加法和乘法同态运算.SWHE 是众多全同态加密算法的设计基础,针对 FHE 计算性能短期内难以显著提升的状况,现阶段也可将其视作一种初步的替代技术.常见的同态加密方案包括:支持加法同态的 Benaloh[91]和 Paillier 算法[92],支持乘法同态的 RSA[93]和 ElGamal 算法[94],以及支持比特异或同态的 Goldwasser Micali 算法[95]等.

3.2.2 保序加密技术

常见的同态加密算法一般仅支持加法同态或者乘法同态,并不具备密文比较的能力.保序加密(order preserving encryption,简称 OPE)是一类保持明文顺序的密码技术,能够简单且高效地对加密后的数值数据进行比值或排序.若加密函数 $E:X\to Y$ 满足以下条件,则称其具有保序性:

$$\forall x_1, x_2 \in X, x_1 < x_2 \text{ iff } E(x_1) < E(x_2).$$

2004 年,Agrawal 等人[96]提出首个保序加密算法,使得在不解密的情况下对加密数据库的精确查询成为可能.加密过程是将明文映射到某一目标分布区间.该方案时空开销合理,可以处理明文空间的增量更新,却未给出任何安全性分析.2009 年,基于超几何分布的伪随机对称保序加密算法 SE[97]被提出,首次证明 OPE 能够抵御弱选择明文攻击.随后,Xiao 等人[98]围绕 SE 算法中 idea 模型的信息泄露展开研究,并计算出攻击成功的上限概率.mOPE[99]是一种交互式安全协议,达到了理想化的 IND-OCPA 安全.Papa 等人[99]指出密文可变性是设计安全 OPE 方案时必须考虑的首要因素.此外,OPE 语义安全[100]也是近年来研究的热点问题.

传统 OPE 算法主要基于多项式函数或桶划分操作,必须预先已知全部输入明文值的分布情况.因此,对于大规模动态数据集,算法的可扩展性、效率与准确性尚待提高.近期,Krendelev 等人[101]基于矩阵和算术编码技术分别设计了 OPE 方案,密码强度进一步得到改善.引入随机噪声的 OPE 算法[102]的拟线性加密结构导致较差的安全性.扩展消息空间[103]可以解决此问题,并且抵御唯密文攻击与特定的选择明文攻击.确定性 OPE 加密算法严重威胁明文域的安全,特别是其中基于公钥密码的 OPE 方案通过折半查找极易被破解,解决方法是以一定的概率将明文数值映射为某一区间内的随机数.例如:Reddy 和 Ramachandram 在 mOPE 方案[99]的研究基础上,提出了随机化的 ROPE 方案[104],确保这种随机加密方式不会泄露除大小关系之外的任何信息.相关的随机性加密方案还包括 MV-POPES[105]等.目前,不存在能够同时支持保序加密与同态加密的算法,且 OPE 方案的安全性仍然缺少严格的证明,限制了保序加密技术在云计算环境中的应用.

3.2.3 安全外包方案

云计算用户通过将大规模计算问题外包给 CSP 以降低自身的计算、存储与维护开销,并改善用户操作的灵活性、性价比与服务质量.安全外包(secure outsourcing)的首要目标是保护外包数据的隐私.隐私保护外包计算的一般化流程如图 4 所示.一个或多个资源受限的数据源将各自产生或收集的数据加密后外包至不可信的第三方服务器,即 CSP.由授权的数据使用者向 CSP 提出具体的计算请求.CSP 执行相应的外包计算后返回计算结果,并由客户端进行解密.

Fig.4 Process of privacy-preserving outsourcing computation

图 4 隐私保护外包计算流程

上述过程的主要难点是如何对加密后的数据进行操作.普通的加密方式在保护数据机密性之外,难以在数据无需解密的前提下支持密文计算.伴随多样的云计算需求的增长,计算模式的不确定性更加剧了隐私保护外包计算方案的设计难度,本节将详细阐述相关的研究现状.同时,由于半可信 CSP 可能存在软件错误、硬件错误、外部攻击等不良状况,或者试图恶意压缩计算成本以谋取更大的经济利益,常常使得用户无法完全信赖 CSP 给

出的计算结果,因此需要加以验证,详见第 3.3 节内容.

现有隐私保护外包计算研究主要分为自底向上的方法和自顶向下的方法.其中,自底向上方法将所有形式的外包计算分解为低级别的电路估值或全同态加密,意图通过严密的理论证明,一次性解决外包计算的隐私性问题.同态加密该项密码学技术自提出以来,先后有众多研究者通过设计不同的安全算法或协议,在各种常见安全假设下实现了外包计算的隐私保护,但是此类方案的实用性通常较差,具体内容详见第 3.2.1 节.自顶向下方法则依次为每个具体而独立的外包计算请求(如数据挖掘、数据搜索、图像视觉、工程计算等领域中的某个算法)设计相应的安全外包解决方案,并权衡安全、功能与效率等属性之间的关系.近期研究成果包括:

对于基本数据库操作或代数运算,已经先后为等值连接查询[106]、多维范围查询[107]、二进制联合查询[108]和相似性查询[109]设计了安全外包计算方案,以及专用于求和[110]、内积[110]、线性方程[111]等运算的外包隐私保护算法.关于密码的外包计算,主要有模幂运算安全外包方案[112]、乱码电路估值安全外包方案[113]等.后者相较非外包的情况,其执行时间与所需带宽分别减少了 98.92%和 99.95%,完全适用于移动平台.此外,人脸识别技术[114]、云协作的移动医疗监控体系 mHealth[115]、恶意域检测服务 DNSRadar[116]等,均广泛应用了隐私保护外包计算技术.

数据挖掘算法是云计算外包的重要应用之一.首先,k 最近邻算法(k-nearest neighbor,简称 kNN)与支持向量机算法(support vector machine,简称 SVM)均是该领域中用于密文搜索与分类的常用工具.Samanthula 等人[117]首次在半可信模型下为 kNN 算法设计了安全外包协议,以保护搜索过程中用户个人数据、查询输入串和访问模式的机密性.Rahulamathavan 等人[118]使用 Pailler 同态加密与两方安全计算,给出了首个基于 SVM 算法的安全密文分类协议.此外,针对一些字符序列的数据挖掘算法,国内外的研究者也提出了相应的安全计算方案,以编辑距离(序列比较)算法为例.该算法目前常见于大规模全基因组测序问题,要以较低的存储开销、合理的查询次数,满足隐私与安全性的需求.

2005 年前后,Atallah 等人[119]首次为编辑距离算法设计了安全外包协议,主要包括序列填充子协议、数据划分子协议与安全表查询子协议,适用于多客户端数据外包至多服务器的情况.由于客户端仅需要参与最后一步的运算,因而改善了计算与通信量.近期,有关方案[120]运用保密交集操作实现安全外包,协议的安全性已在 DDH 假设下得到证明.在效率优化方面,Blanton 团队[121]针对单一数据源的场景,提出了首个不依赖于公钥密码的非交互外包方案.能够在不增加存储空间的条件下,使计算复杂度从 $O(mn\min(m,n))$ 降至 $O(mn)$,并获得了 $O(\min(m,n))$ 的轮复杂度,其中 m 与 n 为字符串长度.文献[122]借助类同态加密技术实现了编辑距离的保密计算,从而解决外包协议交互次数过多的问题.特别地,研究人员[123]利用 M 矩阵对角线元素的非依赖特性实现了并行计算,为动态规划隐私问题提供了一般化的解决思路.实验结果表明,相比原始协议[119],由于无需计算大量的 Paillier 同态加密,故该方案的性能至少提升了一个量级.然而,此类基于电路的方法在执行过程中容易造成计算结果的泄露.

3.2.4 小 结

云计算用户为克服自身资源限制,将私有数据和具体的外包计算请求委托给云服务平台.在安全外包过程中,CSP 面临的主要挑战是如何在保护数据安全与隐私的前提下完成外包计算任务.本节综述了隐私保护外包计算的两类常用加密技术,即同态加密与保序加密,随后介绍了各领域中已知的安全外包计算协议及其执行效果,其中存在很多共性的问题.

(1) 与传统的多方安全计算协议相比,虽然全同态加密技术的速度慢、效率低,但是计算方式却更加灵活,且交互次数显著减少,使得通信复杂度有所降低.随着研究的不断发展,目前全同态加密方案的性能正在逐渐被提升,但与真正的实用化还有较长的距离,现阶段可以使用类同态加密方案作为代替.

(2) 保序加密技术的突出特点是密文数据能够直接进行排序,基本无需用户参与交互,有效降低了密文搜索的难度,但在实际应用中存在较大的安全风险,特别缺乏理论层面的安全性支持.

(3) 现有安全外包技术通常不具备可扩展性,针对某一特定问题设计的外包计算方案难以迁移到其他应用领域,根本的解决途径仍需等待同态加密技术的突破.到目前为止,在多数据源场景、非交互外包协议、抵御

服务器合谋以及外包计算效率等方面,有着较大的研究空间.

3.3 可验证外包计算

可验证外包计算(verifiable outsourcing computation)是指对云外包计算结果正确性的验证.在完成隐私保护的外包计算后,用户接收计算结果并向 CSP 提出验证请求,由 CSP 返回一些证据.用户通过验证该证据,可以判断云计算结果是否准确无误.可验证外包计算的一般化流程如图 5 所示.除正确性保护之外,可验证外包计算有时也具备抗抵赖和防止伪造的特殊功能.近年来,学者们已经提出了多种类型的可验证安全外包计算方案,并且验证的效率正在逐渐被提高.

Fig.5 Process of verifiable outsourcing computation

图 5 可验证外包计算流程

有效验证委托计算结果的正确性可借助可验证同态加密技术[124].Gennaro 等人[125]于 2010 年首次提出了非交互性可验证计算的概念.数年后,该方案依靠代理不经意传输技术被扩展到了多用户环境[126].Parno 等人[127]给出利用属性加密机制构造可验证外包计算方案的一种方法,并允许公开委托与公开验证.2013 年、2014 年,学术界针对各类常见外包算法的可验证性进行了大量的研究.例如:双线性对被引入到多元多项式的安全求值与微分操作中,实现了支持动态更新的公开可验证计算方案[128].在序列比较外包方案的可验证性研究[129]中,用户可以高效判断云服务器是否按照预先约定执行了安全外包协议,并进行了形式化安全分析.此外,有关矩阵乘积、行列式和逆运算的可验证安全外包协议[130]、用于生物特征计算的可验证外包方案[131]、子图相似性搜索结果的验证算法[132]以及位置查询结果的验证方法[133],均是可验证外包计算领域中的最新研究内容.

流数据规模的快速增长为可验证外包计算方案带来了严峻的挑战.例如天气预报、流量管理、市场分析等应用场景,资源受限的数据拥有者通常会连续地收集、产生数据流,并将它们立即外包给云端服务器.此后,CSP 如何为外包计算结果构造有效的证据,使其顺利通过用户检验且无法伪造,是可验证计算中的一个新问题.现有研究已经实现了流数据在分组聚合查询[134]与线性代数查询[135]中的可验证性,并支持数据值动态更新.

综上所述,云环境下的可验证外包计算研究已经取得了一些显著的进展,总体来说仍有许多不足,主要表现在以下几个方面.

(1) 构造可验证签名或对证据进行验证的方式较复杂,给数据拥有者或数据使用者带来了较大的计算开销.线性复杂度应作为部分可验证外包计算方案的设计目标,以提升方案实施的可行性.

(2) 大量的验证操作常常忽略数据动态更新的情况.如何在外包数据发生变化后最大程度地降低用户的重计算量,并提供快速可靠的动态验证方法,应是未来研究的关键.

(3) 研究更多重要的安全外包计算的可验证性,例如图像处理、加密操作、数据挖掘等算法,特别关注方案应具备的公开可验证性、非交互性、多数据源等特征.

3.4 其他云应用安全问题

云计算的应用种类繁多,尚有众多安全与隐私保护问题本文难以全面覆盖.例如:云端的错误诊断技术[136]和过程监控技术[137],以及 E-Learning 系统的云部署模型[138]等.另外,移动平台的云应用安全也是近年来研究的热点问题.2013 年,Lau 等人[139]应用端到端加密算法实现了适用于移动智能设备的云端数据隐私保护系统 M-Aegis.同年,Liu 与 Zhang 等人[140]研究移动云同步服务的安全威胁,并挖掘跨应用程序脚本漏洞.

4 未来研究展望

本文主要围绕云计算安全的最新研究内容展开综述,介绍了近年来代表性的安全威胁与防御技术.通过分析可以看出现有云安全保护方案仍然存在一些不足,未来的科研工作可以更多地关注于以下几点.

1. 云虚拟化安全中提到的各类攻击一般是利用云基础设施在系统管理程序中存在的缺陷,采取不同的攻击方式以提升操作权限或窃取敏感数据.目前相关研究人员提出了针对性的防御策略,主要的局限性包括:

(1) 异常检测技术通常难以抵御特殊类型的安全攻击,如资源释放型攻击和高速隐蔽信道攻击等,而且检测效率有限,检测过程也可能会泄露隐私.

(2) 防御窃取服务攻击需要结合基础设施的差异来设计虚拟机监控方案,特别是研究适用于不同管理程序的监控实例.

(3) 为更好地防御交叉虚拟机边信道攻击,应该更加关注于云迁移过程中的虚拟机攻击形式,例如对工作量、工作时间等隐私信息的恶意窃取.

(4) 设计能够独立于 CSP 的安全防御策略,从而有效限制 CSP 的权限滥用.安全防御过程中也要注意控制防御方案对公有云性能造成的负面影响.

2. 云存储安全一直备受众多研究者的关注,现有研究相对较为广泛,主要的局限性包括:

(1) 数据共享算法对用户身份隐私的保护程度仍需加强.代理重加密算法的单向性、可传递性等特征尚待进一步研究,而属性加密算法用于动态权限管理时的效率通常较差.

(2) 非对称可搜索加密技术易受推理攻击的威胁,且缺乏对多数据源或多关键词检索的支持.云数据库密文搜索的查询效率有待继续优化,并尝试在提供更多查询处理功能的同时提高隐私保护能力,防止敌手利用访问模式或搜索模式窃取机密信息.

(3) 可回收性证明亟需防御文件级或块级的云端数据非法删除,并提高数据更新情况下的审计效率.最新研究方向之一是证明云文件确实按照某种预定格式(如是否压缩等)进行存储.

3. 有关云计算环境中的各类应用,其安全性研究工作有待进一步深入,主要的局限性包括:

(1) 移动平台有限的存储和计算能力限制了云计算的应用,并带来了全新的安全和隐私威胁.因此要着重研究移动智能终端的安全问题,特别是移动云共享应用中的安全漏洞,以及适用于移动云的可扩展的认证访问机制等.

(2) 在可计算加密方面,尚未发现能够同时支持字符串检索和数值数据运算的加密方案.同态加密技术与保序加密技术目前仍处于研究的起步阶段,复杂的数学结构导致实用性较差.

(3) 在安全外包方面,后续研究的重点应放在防御服务器合谋、改善外包计算开销等内容上,并不断扩展隐私保护外包技术与可验证外包技术所支持的运算类型与算法,同时在标准安全模型下给出严密的安全性证明.

综上,为了全面地提升云计算环境的整体安全程度,应该综合运用云虚拟化安全、云数据安全以及云应用安全研究中涉及的多种防御技术或安全机制.目前研究通常专注于云环境中某个特定的安全需求,并为此提出大量的安全保护方案.然而,为每个安全需求分别部署安全防护措施的方式在实际应用中的可行性较差,而且在单独部署的同时也极有可能引入额外的安全风险.因此,未来研究的首要任务是设计全面完整的安全解决方案,以满足公有云计算环境面临的多样安全需求,使得云用户对安全策略的管理方式更加灵活,能够根据自身需要进行协调,从而快速达到目标安全级别.

5 结束语

低廉的计算成本与灵活的配置能力促使云计算产业蓬勃发展.云计算环境中的虚拟化、多租户、共享资源池等技术也带来了特有的安全问题,特别是缺乏控制云服务资源的有效方法,引起了人们对云安全的普遍关注.通过深入分析与对比,可知云计算安全保护工作在国内外已取得较好的研究成果,但是仍有许多遗留问题尚待探讨,需要综合考虑多种安全因素,不断改善防御技术与安全策略.本文重点介绍了云计算中各类已知安全威胁

与隐私泄露风险的产生原因和特点,然后分别围绕云虚拟化安全、云数据安全以及云应用安全展开综述,以期能够为云安全的未来研究做出一些有益的探索.

References:

[1] Khalil IM, Khreishah A, Azeem M. Cloud computing security: A survey. IEEE Computers, 2014,3(1):1−15.

[2] Bodkhe AP, Dhote CA. Cloud computing security: An issue of concern. Int'l Journal of Advanced Research in Computer Science and Software Engineering, 2015,5(4):1337−1342.

[3] Ali M, Khan SU, Vasilakos AV. Security in cloud computing: Opportunities and challenges. Information Sciences, 2015,305:357−383. [doi: 10.1016/j.ins.2015.01.025]

[4] Feng DG, Zhang M, Zhang Y, Xu Z. Study on cloud computing security. Ruan Jian Xue Bao/Journal of Software, 2011,22(1): 71−83 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3958.htm [doi: 10.3724/SP.J.1001.2011.03958]

[5] National Institute of Standards and Technology. The NIST definition of cloud computing. Technical Report, No.800-145, 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[6] Gruschka N, Jensen M. Attack surfaces: A taxonomy for attacks on cloud services. In: Proc. of the 3rd IEEE Int'l Conf. on Cloud Computing (CLOUD 2010). Washington: IEEE Computer Society, 2010. 276−279. [doi: 10.1109/CLOUD.2010.23]

[7] Zhou FF, Goel M, Desnoyers P, Sundaram R. Scheduler vulnerabilities and coordinated attacks in cloud computing. Journal of Computer Security, 2013,21(4):533−559.

[8] Li M, Zha ZL, Zang WY, Yu M, Liu P, Bai K. Detangling resource management functions from the TCB in privacy-preserving virtualization. In: Kutyłowski M, Vaidya J, eds. Proc. of the 19th European Symp. on Research in Computer Security (ESORICS 2014). Springer-Verlag, 2014. 310−325. [doi: 10.1007/978-3-319-11203-9_18]

[9] Szefer J, Keller E, Lee RB, Rexford J. Eliminating the hypervisor attack surface for a more secure cloud. In: Proc. of the 18th ACM Conf. on Computer and Communications Security (CCS 2011). New York: ACM Press, 2011. 401−412. [doi: 10.1145/2046707.2046754]

[10] Varadarajan V, Kooburat T, Farley B, Ristenpart T, Swift MM. Resource-Freeing attacks: Improve your cloud performance (at your neighbor's expense). In: Proc. of the 19th ACM Conf. on Computer and Communications Security (CCS 2012). New York: ACM Press, 2012. 281−292. [doi: 10.1145/2382196.2382228]

[11] Liu ST, Chen YM. Retrospective detection of malware attacks by cloud computing. In: Proc. of the 2010 Int'l Conf. on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC 2010). Washington: IEEE Computer Society, 2010. 510−517. [doi: 10.1109/CyberC.2010.99]

[12] Jarabek C, Barrera D, Aycock J. ThinAV: Truly lightweight mobile cloud-based anti-malware. In: Proc. of the 28th Computer Security Applications Conf. (ACSAC 2012). New York: ACM Press, 2012. 209−218. [doi: 10.1145/2420950.2420983]

[13] Wei L, Reiter MK. Ensuring file authenticity in private DFA evaluation on encrypted files in the cloud. In: Crampton J, Jajodia S, Mayes K, eds. Proc. of the 18th European Symp. on Research in Computer Security (ESORICS 2013). Heidelberg: Springer-Verlag, 2013. 147−163. [doi: 10.1007/978-3-642-40203-6_9]

[14] Aviram A, Hu S, Ford B, Gummadi R. Determinating timing channels in compute clouds. In: Proc. of the 2010 ACM Workshop on Cloud Computing Security (CCSW 2010). New York: ACM Press, 2010. 103−108. [doi: 10.1145/1866835.1866854]

[15] Hlavacs H, Treutner T, Gelas JP, Lefevre L. Energy consumption side-channel attack at virtual machines in a cloud. In: Proc. of the 9th IEEE Int'l Conf. on Dependable, Autonomic and Secure Computing (DASC 2011). Washington: IEEE Computer Society, 2011. 605−612. [doi: 10.1109/DASC.2011.110]

[16] Wu ZY, Xu Z, Wang HN. Whispers in the hyper-space: High-Speed covert channel attacks in the cloud. In: Proc. of the 21st USENIX Security Symp. (SEC 2012). Berkeley: USENIX Association, 2012. 159−173.

[17] Liu FF, Yarom Y, Ge Q, Heiser G, Lee RB. Last-Level cache side-channel attacks are practical. In: Proc. of the 2015 IEEE Symp. on Security and Privacy (S&P 2015). Washington: IEEE Computer Society, 2015. 605−622. [doi: 10.1109/SP.2015.43]

[18] Inci MS, Gulmezoglu B, Irazoqui G, Eisenbarth T, Sunar B. Seriously, get off my cloud! Cross-VM RSA key recovery in a public cloud. IACR Cryptology ePrint Archive Report, No.2015/898, 2015. http://eprint.iacr.org/2015/898

[19] Pattuk E, Kantarcioglu M, Lin ZQ, Ulusoy H. Preventing cryptographic key leakage in cloud virtual machines. In: Proc. of the 23rd USENIX Security Symp. (SEC 2014). Berkeley: USENIX Association, 2014. 703−718.

[20] Varadarajan V, Ristenpart T, Swift M. Scheduler-Based defenses against cross-VM side-channels. In: Proc. of the 23rd USENIX Security Symp. (SEC 2014). Berkeley: USENIX Association, 2014. 687−702.

[21] Rocha F, Correia M. Lucy in the sky without diamonds: Stealing confidential data in the cloud. In: Proc. of the 41st IEEE/IFIP Int'l Conf. on Dependable Systems and Networks Workshops (DSNW 2011). Washington: IEEE Computer Society, 2011. 129−134. [doi: 10.1109/DSNW.2011.5958798]

[22] Molina JAN, Mishra S. Addressing memory exhaustion failures in virtual machines in a cloud environment. In: Proc. of the 43rd IEEE/IFIP Int'l Conf. on Dependable Systems and Networks (DSN 2013). Washington: IEEE Computer Society, 2013. 1−6. [doi: 10.1109/DSN.2013.6575330]

[23] Szefer J, Lee RB. Architectural support for hypervisor-secure virtualization. ACM SIGARCH Computer Architecture News, 2012, 40(1):437−450. [doi: 10.1145/2189750.2151022]

[24] Antunes N, Vieira M. Defending against Web application vulnerabilities. Computer, 2012,45(2):66−72. [doi: 10.1109/MC.2011.259]

[25] Xia YB, Liu YT, Chen HB, Zang BY. Defending against VM rollback attack. In: Proc. of the 42nd IEEE/IFIP Int'l Conf. on Dependable Systems and Networks Workshops (DSNW 2012). Washington: IEEE Computer Society, 2012. 1−5. [doi: 10.1109/DSNW.2012.6264690]

[26] Elphinstone K, Shen YY. Increasing the trustworthiness of commodity hardware through software. In: Proc. of the 43rd IEEE/IFIP Int'l Conf. on Dependable Systems and Networks (DSN 2013). Washington: IEEE Computer Society, 2013. 1−6. [doi: 10.1109/DSN.2013.6575328]

[27] Azab AM, Ning P, Zhang XL. SICE: A hardware-level strongly isolated computing environment for x86 multi-core platforms. In: Proc. of the 18th ACM Conf. on Computer and Communications Security (CCS 2011). New York: ACM Press, 2011. 375−388. [doi: 10.1145/2046707.2046752]

[28] Green M, Ateniese G. Identity-Based proxy re-encryption. In: Katz J, Yung M, eds. LNCS 4521. Heidelberg: Springer-Verlag, 2007. 288−306. [doi: 10.1007/978-3-540-72738-5_19]

[29] Mizuno T, Doi H. Secure and efficient IBE-PKE proxy re-encryption. IEICE Trans. on Fundamentals of Electronics, Communications and Computer Science, 2011,94-A(1):36−44. [doi: 10.1587/transfun.E94.A.36]

[30] Waters B. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In: Halevi S, ed. Proc. of the 29th Int'l Cryptology Conf. (CRYPTO 2009). Heidelberg: Springer-Verlag, 2009. 619−636. [doi: 10.1007/978-3-642-03356-8_36]

[31] Wang HB, Cao ZF, Wang LC. Multi-Use and unidirectional identity-based proxy re-encryption schemes. Information Sciences, 2010,180:4042−4059. [doi: 10.1016/j.ins.2010.06.029]

[32] Shao J, Cao ZF. Multi-Use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption. Information Sciences, 2012,206:83−95. [doi: 10.1016/j.ins.2012.04.013]

[33] Zhao J, Feng DG, Yang L, Ma LR. CCA-Secure type-based proxy re-encryption without pairings. Acta Electronica Sinica, 2011, 39(11):2513−2519 (in Chinese with English abstract).

[34] Wu XX, Xu L, Zhang XW. A certificateless proxy re-encryption scheme for cloud-based data sharing. In: Proc. of the 18th ACM Conf. on Computer and Communications Security (CCS 2011). New York: ACM Press, 2011. 869−871. [doi: 10.1145/2046707.2093514]

[35] Liang KT, Liu JK, Wong DS, Susilo W. An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing. In: Kutylowski M, Vaidya J, eds. Proc. of the 19th European Symp. on Research in Computer Security (ESORICS 2014). Springer-Verlag, 2014. 257−272. [doi: 10.1007/978-3-319-11203-9_15]

[36] Weng J, Deng RH, Ding XH, Chu CK, Lai JZ. Conditional proxy re-encryption secure against chosen-ciphertext attack. In: Proc. of the 4th Int'l Symp. on Information, Computer, and Communications Security (ASIACCS 2009). New York: ACM Press, 2009. 322−332. [doi: 10.1145/1533057.1533100]

[37] Fang LM, Susilo W, Ge CP, Wang JD. Chosen-Ciphertext secure anonymous conditional proxy re-encryption with keyword search. Theoretical Computer Science, 2012,462:39−58. [doi: 10.1016/j.tcs.2012.08.017]

[38] Fang LM, Wang JD, Ge CP, Ren YJ. Fuzzy conditional proxy re-encryption. SCIENCE CHINA Information Sciences, 2015,56(5): 1−13. [doi: 10.1007/s11432-012-4623-6]

[39] Lan CH, Wang CF. A new conditional proxy re-encryption scheme based on secret sharing. Chinese Journal of Computers, 2013, 36(4):895−902 (in Chinese with English abstract).

[40] Liang KT, Susilo W, Liu JK, Wong DS. Efficient and fully CCA secure conditional proxy re-encryption from hierarchical identity-based encryption. The Computer Journal, 2015,58(10):2778−2792. [doi: 10.1093/comjnl/bxv050]

[41] Liang KT, Liu Z, Tan X, Wong DS, Tang CM. A CCA-secure identity-based conditional proxy re-encryption without random oracles. In: Kwon T, Lee MK, Kwon D, eds. LNCS 7839. Heidelberg: Springer-Verlag, 2012. 231−246. [doi: 10.1007/ 978-3-642-37682-5_17]

[42] Shao J, Wei G, Ling Y, Xie M. Identity-Based conditional proxy re-encryption. In: Proc. of the 2011 IEEE Int'l Conf. on Communications (ICC 2011). Washington: IEEE Computer Society, 2011. 1−5. [doi: 10.1109/icc.2011.5962419]

[43] Waters B. Ciphertext-Policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Catalano D, Fazio N, Gennaro R, Nicolosi A, eds. Proc. of the 14th Int'l Conf. on Practice and Theory in Public-Key Cryptography (PKC 2011). Heidelberg: Springer-Verlag, 2011. 53−70. [doi: 10.1007/978-3-642-19379-8_4]

[44] Green M, Hohenberger S, Waters B. Outsourcing the decryption of ABE ciphertexts. In: Proc. of the 20th USENIX Security Symp. (SEC 2011). Berkeley: USENIX Association, 2011. 34−49.

[45] Lai JZ, Deng RH, Guan CW, Weng J. Attribute-Based encryption with verifiable outsourced decryption. IEEE Trans. on Information Forensics and Security, 2013,8(8):1343−1354. [doi: 10.1109/TIFS.2013.2271848]

[46] Zhang YH, Zheng D, Li J, Li H. Attribute directly-revocable attribute-based encryption with constant ciphertext length. Journal of Cryptologic Research, 2014,1(5):465−480 (in Chinese with English abstract).

[47] Horváth M. Attribute-Based encryption optimized for cloud computing. In: Italiano GF, Margaria-Steffen T, Pokomy J, Quisquater JJ, Wattenhofer R, eds. Proc. of the 41st Int'l Conf. on Current Trends in Theory and Practice of Computer Science (SOFSEM 2015). Heidelberg: Springer-Verlag, 2015. 566−577. [doi: 10.1007/978-3-662-46078-8_47]

[48] Goyal V, Pandey O, Sahai A, Waters B. Attribute-Based encryption for fine-grained access control of encrypted data. In: Proc. of the 13rd ACM Conf. on Computer and Communications Security (CCS 2006). New York: ACM Press, 2006. 89−98. [doi: 10.1145/1180405.1180418]

[49] Attrapadung N, Herranz J, Laguillaumie F, Libert B, Panafieu ED, Råfols C. Attribute-Based encryption schemes with constant-size ciphertexts. Theoretical Computer Science, 2012,422:15−38. [doi: 10.1016/j.tcs.2011.12.004]

[50] Wang CJ, Luo JF. An efficient key-policy attribute-based encryption scheme with constant ciphertext length. Mathematical Problems in Engineering, 2013. 1−7. [doi: 10.1155/2013/810969]

[51] Hohenberger S, Waters B. Attribute-Based encryption with fast decryption. In: Kurosawa K, Hanaoka G, eds. Proc. of the 16th Int'l Conf. on Practice and Theory in Public-Key Cryptography (PKC 2013). Heidelberg: Springer-Verlag, 2013. 162−179. [doi: 10.1007/978-3-642-36362-7_11]

[52] Ambrosin M, Conti M, Dargahi T. On the feasibility of attribute-based encryption on smartphone devices. In: Proc. of the 1st Int'l Workshop on IoT Challenges in Mobile and Industrial Systems (IoT-Sys 2015). New York: ACM Press, 2015. 49−54. [doi: 10.1145/2753476.2753482]

[53] Albeshri A, Caelli W. Mutual protection in a cloud computing environment. In: Proc. of the 12th IEEE Int'l Conf. on High Performance Computing and Communications (HPCC 2010). Washington: IEEE Computer Society, 2010. 641−646. [doi: 10.1109/HPCC.2010.87]

[54] Leandro MAP, Nascimento TJ, dos Santos DR, Westphall CM, Westphall CB. Multi-Tenancy authorization system with federated identity for cloud-based environments using shibboleth. In: Proc. of the 11th Int'l Conf. on Networks (ICN 2012). Saint Gilles: Int'l Academy, Research, and Industry Association, 2012. 88−93.

[55] Kuhn DR, Coyne EJ, Weil TR. Adding attributes to role based access control. IEEE Computers, 2010,43(6):79−81. [doi: 10.1109/MC.2010.155]

[56] Bijon KZ, Krishnan R, Sandhu R. Risk-Aware RBAC sessions. In: Venkatakrishnan V, Goswami D, eds. LNCS 7671. Heidelberg: Springer-Verlag, 2012. 59−74. [doi: 10.1007/978-3-642-35130-3_5]

[57] Lang X, Wei LX, Wang XA, Wu XG. Cryptographic access control scheme for cloud storage based on proxy re-encryption. Journal of Computer Applications, 2014,34(3):724−727 (in Chinese with English abstract). http://dx.chinadoi.cn/10.11772/j.issn.1001-9081.2014.03.0724

[58] Marcon AL, Santin AO, Stihler M, Bachtold J. A $UCON_{ABC}$ resilient authorization evaluation for cloud computing. IEEE Trans. on Parallel and Distributed Systems, 2013,25(2):457−467. [doi: 10.1109/TPDS.2013.113]

[59] Song DX, Wagner D, Perrig A. Practical techniques for searches on encrypted data. In: Proc. of 2010 IEEE Symp. on Security and Privacy (S&P 2010). Washington: IEEE Computer Society, 2000. 44−55. [doi: 10.1109/SECPRI.2000.848445]

[60] Lu YB. Privacy-Preserving logarithmic-time search on encrypted data in cloud. In: Proc. of the 19th Network and Distributed System Security Symp. (NDSS 2012). Reston: The Internet Society, 2012. 1−17.

[61] Strizhov M, Ray I. Multi-Keyword similarity search over encrypted cloud data. In: Cuppens-Boulahia N, Cuppens F, Jajodia S, Kalam AAE, Sans T, eds. Proc. of the 29th IFIP TC 11 Int'l Conf. (IFIP SEC 2014). Heidelberg: Springer-Verlag, 2014. 52−65. [doi: 10.1007/978-3-642-55415-5_5]

[62] Liu C, Zhu LH, Chen JJ. Efficient searchable symmetric encryption for storing multiple source data on cloud. IACR Cryptology ePrint Archive Report, No. 2015/349, 2015. http://eprint.iacr.org/2015/349

[63] Li JG, Shi YR, Zhang YC. Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage. Int'l Journal of Communication Systems, 2015. [doi: 10.1002/dac.2942]

[64] Rompay CV, Molva R, Önen M. Multi-User searchable encryption in the cloud. In: Lopez J, Mitchell CJ, eds. LNCS 9290. Springer-Verlag, 2015. 299−316. [doi: 10.1007/978-3-319-23318-5_17]

[65] Boneh D, Waters B. Conjunctive, subset, and range queries on encrypted data. In: Proc. of the 4th Theory of Cryptography Conf. (TCC 2007). Heidelberg: Springer-Verlag, 2007. 535−554. [doi: 10.1007/978-3-540-70936-7_29]

[66] Baek J, Safavi-Naini R, Susilo W. Public key encryption with keyword search revisited. In: Gervasi O, Murgante B, Laganà A, Taniar D, Mun Y, Gavrilova ML, eds. LNCS 5072. Heidelberg: Springer-Verlag, 2008. 1249−1259. [doi: 10.1007/978-3-540-69839-5_96]

[67] Katz J, Sahai A, Waters B. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart N, ed. Advances in Cryptology–EUROCRYPT 2008. Heidelberg: Springer-Verlag, 2008. 146−162. [doi: 10.1007/978-3-540-78967-3_9]

[68] Li J, Wang Q, Wang C, Cao N, Ren K, Lou WJ. Fuzzy keyword search over encrypted data in cloud computing. In: Proc. of the 29th IEEE Int'l Conf. on Computer Communications (INFOCOM 2010). Piscataway: IEEE Press, 2010. 441−445. [doi: 10.1109/INFCOM.2010.5462196]

[69] Cloud Security Alliance. The notorious nine cloud computing top threats in 2013. Technical Report, 2013. http://www.chinacloud.cn/upload/2013-03/13030711513081.pdf

[70] Juels A, Kaliski B. Pors: Proofs of retrievability for large files. In: Ning P, Vimercati SDC, Syverson PF, eds. Proc. of the 14th ACM Conf. on Computer and Communications Security (CCS 2007). New York: ACM Press, 2007. 584−597. [doi: 10.1145/1315245.1315317]

[71] Zeng K. Publicly verifiable remote data integrity. In: Chen LQ, Ryan MD, Wang GL, eds. LNCS 5308. Heidelberg: Springer-Verlag, 2008. 419−434. [doi: 10.1007/978-3-540-88625-9_28]

[72] Li J, Tan X, Chen XF, Wong DS, Xhafa F. OPoR: Enabling proof of retrievability in cloud computing with resource-constrained devices. IEEE Trans. on Cloud Computing, 2015,3(2):195−205. [doi: 10.1109/TCC.2014.2366148]

[73] Yun A, Shi C, Kim Y. On protecting integrity and confidentiality of cryptographic file system for outsourced storage. In: Sion R, ed. Proc. of the 2009 ACM Workshop on Cloud Computing Security (CCSW 2009). New York: ACM Press, 2009. 67−76. [doi: 10.1145/1655008.1655017]

[74] Wang Q, Wang C, Li J, Ren K, Lou W. Enabling public verifiability and data dynamics for storage security in cloud computing. In: Backes M, Ning P, eds. Proc. of the 14th European Symp. on Research in Computer Security (ESORICS 2009). Heidelberg: Springer-Verlag, 2009. 355−370. [doi: 10.1007/978-3-642-04444-1_22]

[75] Ateniese G, Burns R, Curtmola R, Herring J, Kissner L, Peterson Z, Song D. Provable data possession at untrusted stores. In: Ning P, Vimercati SDC, Syverson PF, eds. Proc. of the 14th ACM Conf. on Computer and Communications Security (CCS 2007). New York: ACM Press, 2007. 598−609. [doi: 10.1145/1315245.1315318]

[76] Barsoum AF, Hasan MA. Provable multicopy dynamic data possession in cloud computing systems. IEEE Trans. on Information Forensics and Security, 2015,10(3):485−497. [doi: 10.1109/TIFS.2014.2384391]

[77] Wang HQ. Identity-Based distributed provable data possession in multicloud storage. IEEE Trans. on Services Computing, 2015, 8(2):328−340. [doi: 10.1109/TSC.2014.1]

[78] Karnwal T, Sivakumar T, Aghila G. A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack. In: Proc. of the 2012 IEEE Students' Conf. on Electrical, Electronics and Computer Science (SCEECS 2012). Washington: IEEE Computer Society, 2012. 1−5. [doi: 10.1109/SCEECS.2012.6184829]

[79] Slopek A, Vlajic N. Economic denial of sustainability (EDoS) attack in the cloud using Web-bugs. In: Proc. of the 17th Int'l Symp. on Research in Attacks, Intrusions, and Defenses (RAID 2014). Springer-Verlag, 2014. 469−471.

[80] Zhao S, Lee PPC, Lui JCS, Guan XH, Ma XB, Tao J. Cloud-Based push-styled mobile botnets: A case study of exploiting the cloud to device messaging service. In: Proc. of the 28th Computer Security Applications Conf. (ACSAC 2012). New York: ACM Press, 2012. 119−128. [doi: 10.1145/2420950.2420968]

[81] Lin WJ, Lee D. Traceback attacks in cloud-Pebbletrace botnet. In: Proc. of the 32nd Int'l Conf. on Distributed Computing Systems Workshops (ICDCSW 2012). Washington: IEEE Computer Society, 2012. 417−426. [doi: 10.1109/ICDCSW.2012.61]

[82] Kourai K, Azumi T, Chiba S. A self-protection mechanism against stepping-stone attacks for IaaS clouds. In: Proc. of the 9th Int'l Conf. on Ubiquitous Intelligence & Computing and the 9th Int'l Conf. on Autonomic & Trusted Computing (UIC/ATC 2012). Washington: IEEE Computer Society, 2012. 539−546. [doi: 10.1109/UIC-ATC.2012.139]

[83] Hasna POH. Audio steganography scheme to advance the security of data in hybrid cloud. Int'l Journal of Advanced Research in Computer and Communication Engineering, 2015,4(1):73−75.

[84] Liu B, Xu E, Wang J, Wei ZL. Thwarting audio steganography attacks in cloud storage systems. In: Proc. of the 2011 Int'l Conf. on Cloud and Service Computing (CSC 2011). Washington: IEEE Computer Society, 2011. 259−265. [doi: 10.1109/CSC.2011.6138530]

[85] Gentry C. Fully homomorphic encryption using ideal lattices. In: Proc. of the 41st ACM Symp. on Theory of Computing (STOC 2009). New York: ACM Press, 2009. 169−178. [doi: 10.1145/1536414.1536440]

[86] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE. In: Proc. of the 52nd IEEE Symp. on Foundations of Computer Science (FOCS 2011). Washington: IEEE Computer Society, 2011. 97−106. [doi: 10.1109/FOCS.2011.12]

[87] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping. In: Proc. of the 3rd Innovations in Theoretical Computer Science Conf. (ITCS 2012). New York: ACM Press, 2012. 309−325. [doi: 10.1145/2090236.2090262]

[88] Gennaro R, Wichs D. Fully homomorphic message authenticators. In: Sako K, Sarkar P, eds. Proc. of the 19th Int'l Conf. on the Theory and Application of Cryptology and Information Security (Asiacrypt 2013). Heidelberg: Springer-Verlag, 2013. 301−320. [doi: 10.1007/978-3-642-42045-0_16]

[89] Boneh D, Freeman DM. Homomorphic signatures for polynomial functions. In: Paterson KG, ed. Advances in Cryptology—EUROCRYPT 2011. Heidelberg: Springer-Verlag, 2011. 149−168. [doi: 10.1007/978-3-642-20465-4_10]

[90] Catalano D, Fiore D, Warinschi B. Homomorphic signatures with efficient verification for polynomial functions. In: Garay JA, Gennaro R, eds. Proc. of the 34th Int'l Cryptology Conf. (CRYPTO 2014). Heidelberg: Springer-Verlag, 2014. 371−389. [doi: 10.1007/978-3-662-44371-2_21]

[91] Benaloh J. Verifiable secret-ballot elections [Ph.D. Thesis]. New Haven: Yale University, 1988.

[92] Paillier P. Public-Key cryptosystems based on composite degree residuosity classes. In: Stern J, ed. Advances in Cryptology—EUROCRYPT 1999. Heidelberg: Springer-Verlag, 1999. 223−238. [doi: 10.1007/3-540-48910-X_16]

[93] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978,21(2):120−126. [doi: 10.1145/359340.359342]

[94] Elgamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. on Information Theory, 1985,31(4):469−472. [doi: 10.1109/TIT.1985.1057074]

[95] Goldwasser S, Micali S. Probabilistic encryption and how to play mental poker keeping secret all partial information. In: Proc. of the 14th ACM Symp. on Theory of Computing (STOC 1982). New York: ACM Press, 1982. 365−377. [doi: 10.1145/800070.802212]

[96] Agrawal R, Kiernan J, Srikant R, Xu YR. Order preserving encryption for numeric data. In: Proc. of the 2004 ACM Special Interest Group on Management of Data (SIGMOD 2004). New York: ACM Press, 2004. 563−574. [doi: 10.1145/1007568.1007632]

[97] Boldyreva A, Chenette N, Lee Y, O'Neill A. Order-Preserving symmetric encryption. In: Joux A, ed. Advances in Cryptology—EUROCRYPT 2009. Heidelberg: Springer-Verlag, 2009. 224−241. [doi: 10.1007/978-3-642-01001-9_13]

[98] Xiao LL, Yen I-L, Lin DD. Security analysis for an order preserving encryption scheme. In: Proc. of the 46th Conf. on Information Sciences and Systems (CISS 2012). Washington: IEEE Computer Society, 2012. 1−6. [doi: 10.1109/CISS.2012.6310814]

[99] Popa RA, Li FH, Zeldovich N. An ideal-security protocol for order preserving encoding. In: Proc. of the 2013 IEEE Symp. on Security and Privacy (S&P 2013). Washington: IEEE Computer Society, 2013. 463−477. [doi: 10.1109/SP.2013.38]

[100] Boneh D, Lewi K, Raykova M, Sahai A, Zhandry M, Zimmerman J. Semantically secure order-revealing encryption: Multi-Input functional encryption without obfuscation. In: Oswald E, Fischlin M, eds. Advances in Cryptology—EUROCRYPT 2015. Heidelberg: Springer-Verlag, 2015. 563−594. [doi: 10.1007/978-3-662-46803-6_19]

[101] Krendelev SF, Yakovlev M, Usoltseva M. Order-Preserving encryption schemes based on arithmetic coding and matrices. In: Proc. of the 2014 Federated Conf. on Computer Science and Information Systems (FedCSIS 2014). Washington: IEEE Computer Society, 2014. 891−899. [doi: 10.15439/2014F186]

[102] Liu DX, Wang SL. Programmable order-preserving secure index for encrypted database query. In: Proc. of the 5th IEEE Int'l Conf. on Cloud Computing (CLOUD 2012). Washington: IEEE Computer Society, 2012. 502−509. [doi: 10.1109/CLOUD.2012.65]

[103] Liu ZL, Chen XF, Yang J, Jia CF, You L. New order preserving encryption model for outsourced databases in cloud environments. Journal of Network and Computer Applications, 2016,59:198−207. [doi: 10.1016/j.jnca.2014.07.001]

[104] Reddy KS, Ramachandram S. A new randomized order preserving encryption scheme. Int'l Journal of Computer Applications, 2014,108(12):41−46. [doi: 10.5120/18967-0310]

[105] Kadhem H, Amagasa T, Kitagawa H. MV-OPES: Multivalued-Order preserving encryption scheme: A novel scheme for encrypting integer value to many different values. IEICE Trans. on Information and Systems, 2010,E93-D(9):2520−2533. [doi: 10.1587/transinf.E93.D.2520]

[106] Pang H, Ding XH. Privacy-Preserving ad-hoc equi-join on outsourced data. ACM Trans. on Database Systems, 2014,39(3):1−40. [doi: 10.1145/2629501]

[107] Hore B, Mehrotra S, Canim M, Kantarcioglu M. Secure multidimensional range queries over outsourced data. VLDB Journal, 2012, 21(3):333−358. [doi: 10.1007/s00778-011-0245-7]

[108] Carbunar B, Sion R. Toward private joins on outsourced data. IEEE Trans. on Knowledge and Data Engineering, 2012,24(9):1699−1710. [doi: 10.1109/TKDE.2011.142]

[109] Yiu ML, Assent I, Jensen CS, Kalnis P. Outsourced similarity search on metric data assets. IEEE Trans. on Knowledge and Data Engineering, 2012,24(2):338−352. [doi: 10.1109/TKDE.2010.222]

[110] Jung T, Li XY, Wan M. Collusion-Tolerable privacy-preserving sum and product calculation without secure channel. IEEE Trans. on Dependable and Secure Computing, 2014,12(1):45−57. [doi: 10.1109/TDSC.2014.2309134]

[111] Chen XF, Huang XY, Li J, Ma JF, Lou WJ, Wong DS. New algorithms for secure outsourcing of large-scale systems of linear equations. IEEE Trans. on Information Forensics and Security, 2014,10(1):69−78. [doi: 10.1109/TIFS.2014.2363765]

[112] Chen XF, Li J, Ma JF, Tang Q, Lou WJ. New algorithms for secure outsourcing of modular exponentiations. In: Foresti S, Yung M, Martinelli F, eds. Proc. of the 17th European Symp. on Research in Computer Security (ESORICS 2012). Heidelberg: Springer-Verlag, 2012. 541−556. [doi: 10.1007/978-3-642-33167-1_31]

[113] Carter H, Mood B, Traynor P, Butler K. Secure outsourced garbled circuit evaluation for mobile devices. In: Proc. of the 22nd USENIX Security Symp. (SEC 2013). Berkeley: USENIX Association, 2013. 289−304.

[114] Troncoso-Pastoriza JR, González-Jiménez D, Pérez-González F. Fully private noninteractive face verification. IEEE Trans. on Information Forensics and Security, 2013,8(7):1101−1114. [doi: 10.1109/TIFS.2013.2262273]

[115] Lin H, Shao J, Zhang C, Fang YG. CAM: Cloud-Assisted privacy preserving mobile health monitoring. IEEE Trans. on Information Forensics and Security, 2013,8(6):985−997. [doi: 10.1109/TIFS.2013.2255593]

[116] Ma XB, Zhang JJ, Tao J, Li JF, Tian J, Guan XH. DNSRadar: Outsourcing malicious domain detection based on distributed cache-footprints. IEEE Trans. on Information Forensics and Security, 2014,9(11):1906−1921. [doi: 10.1109/TIFS.2014.2357251]

[117] Samanthula BK, Elmehdwi Y, Jiang W. *K*-Nearest neighbor classification over semantically secure encrypted relational data. IEEE Trans. on Knowledge and Data Engineering, 2014,27(5):1261−1273. [doi: 10.1109/TKDE.2014.2364027]

[118] Rahulamathavan Y, Phan RCW, Veluru S, Cumanan K, Rajarajan M. Privacy-Preserving multi-class support vector machine for outsourcing the data classification in cloud. IEEE Trans. on Dependable and Secure Computing, 2013,11(5):467−479. [doi: 10.1109/TDSC.2013.51]

[119] Atallah MJ, Li JT. Secure outsourcing of sequence comparisons. Int'l Journal of Information Security, 2005,4(4):277−287. [doi: 10.1007/s10207-005-0070-3]

[120] Baldi P, Baronio R, Cristofaro ED, Gasti P, Tsudik G. Countering GATTACA: Efficient and secure testing of fully-sequenced human genomes. In: Proc. of the 18th ACM Conf. on Computer and Communications Security (CCS 2011). New York: ACM Press, 2011. 691−702. [doi: 10.1145/2046707.2046785]

[121] Blanton M, Atallah MJ, Frikken KB, Malluhi Q. Secure and efficient outsourcing of sequence comparisons. In: Foresti S, Yung M, Martinelli F, eds. Proc. of the 17th European Symp. on Research in Computer Security (ESORICS 2012). Heidelberg: Springer-Verlag, 2012. 505−522. [doi: 10.1007/978-3-642-33167-1_29]

[122] Cheon JH, Kim M, Lauter K. Homomorphic computation of edit distance. In: Brenner M, Christin N, Johnson B, Rohloff K, eds. Proc. of the 2015 Int'l Workshops on Financial Cryptography and Data Security (FC 2015). Heidelberg: Springer-Verlag, 2015. 194−212. [doi: 10.1007/978-3-662-48051-9_15]

[123] Jha S, Kruger L, Shmatikov V. Toward practical privacy for genomic computation. In: Proc. of the 2008 IEEE Symp. on Security and Privacy (S&P 2008). Washington: IEEE Computer Society, 2008. 216−230. [doi: 10.1109/SP.2008.34]

[124] Lai JZ, Deng RH, Pang H, Weng J. Verifiable computation on outsourced encrypted data. In: Kutylowski M, Vaidya J, eds. Proc. of the 19th European Symp. on Research in Computer Security (ESORICS 2014). Springer-Verlag, 2014. 273−291. [doi: 10.1007/978-3-319-11203-9_16]

[125] Gennaro R, Gentry C, Parno B. Non-Interactive verifiable computing: outsourcing computation to untrusted workers. In: Rabin T, ed. Proc. of the 30th Int'l Cryptology Conf. (CRYPTO 2010). Heidelberg: Springer-Verlag, 2010. 465−482. [doi: 10.1007/978-3-642-14623-7_25]

[126] Choi SG, Katz J, Kumaresan R, Cid C. Multi-Client non-interactive verifiable computation. In: Sahai A, ed. Proc. of the 10th Theory of Cryptography Conf. (TCC 2013). Heidelberg: Springer-Verlag, 2013. 499−518. [doi: 10.1007/978-3-642-36594-2_28]

[127] Parno B, Raykova M, Vaikuntanathan V. How to delegate and verify in public: Verifiable computation from attribute-based encryption. In: Cramer R, ed. Proc. of the 9th Theory of Cryptography Conf. (TCC 2012). Heidelberg: Springer-Verlag, 2012. 422−439. [doi: 10.1007/978-3-642-28914-9_24]

[128] Papamanthou C, Shi E, Tamassia R. Signatures of correct computation. In: Sahai A, ed. Proc. of the 10th Theory of Cryptography Conf. (TCC 2013). Heidelberg: Springer-Verlag, 2013. 222−242. [doi: 10.1007/978-3-642-36594-2_13]

[129] Feng YS, Ma H, Chen XF, Zhu H. Secure and verifiable outsourcing of sequence comparisons. In: Mustofa K, Neuhold EJ, Tjoa AM, Weippl E, You I, eds. LNCS 7804. Heidelberg: Springer-Verlag, 2013. 243−252. [doi: 10.1007/978-3-642-36818-9_25]

[130] Hu X, Pei DY, Tang CM, Wong DS. Verifiable and secure outsourcing of matrix calculation and its application. Science China Information Sciences, 2013,43(7):842−852 (in Chinese with English abstract).

[131] Blanton M, Zhang YH, Frikken KB. Secure and verifiable outsourcing of large-scale biometric computations. ACM Trans. on Information and System Security, 2014,16(3):11−33. [doi: 10.1145/2535523]

[132] Peng Y, Fan Z, Choi B, Xu JL. Authenticated subgraph similarity search in outsourced graph databases. IEEE Trans. on Knowledge and Data Engineering, 2014,27(7):1838−1860. [doi: 10.1109/TKDE.2014.2316818]

[133] Lin X, Xu JL, Hu HB, Lee WC. Authenticating location-based skyline queries in arbitrary subspaces. IEEE Trans. on Knowledge and Data Engineering, 2014,26(6):1479−1493. [doi: 10.1109/TKDE.2013.137]

[134] Nath S, Venkatesan R. Publicly verifiable grouped aggregation queries on outsourced data streams. In: Proc. of the 29th IEEE Int'l Conf. on Data Engineering (ICDE 2013). Washington: IEEE Computer Society, 2013. 517−528. [doi: 10.1109/ICDE.2013.6544852]

[135] Stavros P, Cormode G, Deligiannakis A, Garofalakis M. Lightweight authentication of linear algebraic queries on data streams. In: Proc. of the 2013 ACM Special Interest Group on Management of Data (SIGMOD 2013). New York: ACM Press, 2013. 881−892. [doi: 10.1145/2463676.2465281]

[136] Xu XW, Zhu LM, Weber I, Bass L, Sun D. POD-Diagnosis: Error diagnosis of sporadic operations on cloud applications. In: Proc. of the 44th IEEE/IFIP Int'l Conf. on Dependable Systems and Networks (DSN 2014). Washington: IEEE Computer Society, 2014. 252−263. [doi: 10.1109/DSN.2014.94]

[137] Srinivasan D, Wang Z, Jiang XX, Xu DY. Process out-grafting: An efficient 'out-of-VM' approach for fine-grained process execution monitoring. In: Proc. of the 18th ACM Conf. on Computer and Communications Security (CCS 2011). New York: ACM Press, 2011. 363−374. [doi: 10.1145/2046707.2046751]

[138] Leloglu E, Ayav T, Aslan BG. A review of cloud deployment models for e-learning systems. In: Proc. of the 43rd IEEE/IFIP Int'l Conf. on Dependable Systems and Networks (DSN 2013). Washington: IEEE Computer Society, 2013. 1−2. [doi: 10.1109/DSN.2013.6575331]

[139] Lau B, Chung S, Song CY, Jang Y, Lee W, Boldyreva A. Mimesis aegis: A mimicry privacy Shield-a system's approach to data privacy on public cloud. In: Proc. of the 23rd USENIX Security Symp. (SEC 2014). Berkeley: USENIX Association, 2014. 33−48.

[140] Liu QX, Zhang YQ, Cao C, Wen GX. Cloud synchronization increase cross-application scripting threats on smartphone. In: Proc. of the 16th Int'l Symp. on Research in Attacks, Intrusions, and Defenses (RAID 2013). Heidelberg: Springer-Verlag, 2013. 465−466.

附中文参考文献:

[4] 冯登国,张敏,张妍,徐震.云计算安全研究.软件学报,2011,22(1):71−83. http://www.jos.org.cn/1000-9825/3958.htm [doi: 10.3724/SP.J.1001.2011.03958]

[33] 赵菁,冯登国,杨林,马琳茹.一个高效的选择密文安全的分类代理重加密方案.电子学报,2011,39(11):2513−2519.

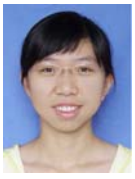
[39] 蓝才会,王彩芬.一个新的基于秘密共享的条件代理重加密方案.计算机学报,2013,36(4):895−902.

[46] 张应辉,郑东,李进,李晖.密文长度恒定且属性直接可撤销的基于属性的加密.密码学报,2014,1(5):465−480.

[57] 郎讯,魏立线,王绪安,吴旭光.基于代理重加密的云存储密文访问控制方案.计算机应用,2014,34(3):724−727. http://dx.chinadoi.cn/10.11772/j.issn.1001-9081.2014.03.0724

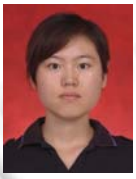
[130] 胡杏,裴定一,唐春明,Wong DS.可验证安全外包矩阵计算及其应用.中国科学:信息科学,2013,43(7):842−852.

张玉清(1966－),男,陕西宝鸡人,博士,教授,博士生导师,主要研究领域为网络与信息系统安全.



王晓菲(1990－),女,博士生,主要研究领域为云计算安全.

刘雪峰(1985－),男,博士,讲师,主要研究领域为云计算安全.



刘玲(1991－),女,博士生,主要研究领域为云计算安全.